# CSfC Selections for Certificate Authorities

Certificate Authorities used in CSfC solutions shall be validated by NIAP/CCEVS or CCRA partnering schemes as complying with the current requirements of NIAP's Protection Profile for Certification Authorities. This validated compliance shall include the selectable requirements contained in this document.

## CSfC selections for Certificate Authority evaluations:

**FCS_CKM.1.1(1)**: The TSF shall generate asymmetric cryptographic keys used for key establishment in accordance with:

- *NIST Special Publication 800-56A, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography" for elliptic curve-based key establishment schemes and implementing "NIST curves" P-256, P-384 and[selection: P-521, no other curves] (as defined in FIPS PUB 186-4, "Digital Signature Standard")*

**FCS_CKM.1.1(2)** The TSF shall generate asymmetric cryptographic keys used for authentication in accordance with a specified cryptographic key generation algorithm

- *FIPS PUB 186-4, "Digital Signature Standard (DSS)", Appendix B.4 for ECDSA schemes and implementing "NIST curves" P-256, P-384 and [selection: P-521, no other curves]*

FCS_COP.1.1(1) **Refinement:** The TSF and [selection: TOE environment, no other component] shall perform [*encryption and decryption*] in accordance with a specified cryptographic algorithm:

- AES-CBC (as defined in NIST SP 800-38A) mode
- AES-GCM (as defined in NIST SP 800-38D) mode,

and cryptographic key size 128-bit key size and [256-bit key size].

FCS_COP.1.1(2) **Refinement:** The TSF and [selection: TOE environment no other component] shall perform **cryptographic signature services** in accordance with the following specified cryptographic algorithms

- Elliptic Curve Digital Signature Algorithm (ECDSA) with a key size of 256 bits or greater that meets FIPS PUB 186-4, "Digital Signature Standard" with "NIST curves" P-256, P-384 and [selection: P-521, no other curves] (as defined in FIPS PUB 186-4, "Digital Signature Standard")

FCS_COP.1.1(3) **Refinement:** The TSF and [selection: TOE environment, no other component] shall perform [*cryptographic hashing services*] in accordance with a specified cryptographic algorithm [**SHA-256, SHA-384**] **and message digest sizes** [**256, 384**] **bits** that meet the following: *FIPS Pub 180-4, "Secure Hash Standard."*

FCS_RBG_EXT.1.2 The deterministic RBG shall be seeded by an entropy source that accumulates entropy from [selection: <u>a software-based noise source, TSF hardware-based noise source</u>] with a minimum of [<u>256 bits</u>] of entropy at least equal to the greatest security strength (according to NIST SP 800-57) of the keys and authorization factors that it will generate.